

ERIC S. CLARK, Individually and on
Behalf of All Others Similarly Situated,

Plaintiff,

vs.

EXCELLUS HEALTH PLAN, INC.,

Defendant

DEMAND FOR JURY TRIAL

FACTUAL SUMMARY

- 1

3. Excellus collected PII from non-subscribers as well. In some instances, individuals treating with an Excellus-affiliated health care provider who are not insured by Excellus, provided their PII in order to obtain treatment. In other instances, Excellus collected PII from individuals whose employers collected PII and provided it to Excellus, even though the employee elected not to be insured by Excellus.

4. On September 9, 2015, Excellus announced a massive data breach that affected the PII of approximately 10 million persons. According to Excellus, it believed that the breach began in December, 2013, and went undetected for nearly two years. Excellus further claimed that it learned of the data breach on August 5, 2015, but did not inform its customers or anyone else who's PII it collected, until September 9, 2015.

5. Uniquely sensitive PII belonging to Plaintiff and other Class members has now been compromised. This enables criminals, not only those who masterminded the hack, but also anyone who may have purchased the PII from them, to fraudulently obtain credit cards, issue fraudulent checks, liquidate existing investment accounts and open new ones. The potential for future theft is great in this instance because the PII theft included social security numbers.

6. In light of the breach, Excellus has offered affected customers and those who's PII it collected, two years of identity theft protection services through Kroll. Those remedial measures are inadequate, as Plaintiff and other Class members will be vulnerable to identity theft for the remainder of their lives, as their social security numbers will not change.

PARTIES

13. Plaintiff, Eric Clark, resides in Waterford, New York. Plaintiff Clark is not insured by Excellus Blue Cross Blue Shield, but Excellus obtained Plaintiff Clark's PII from his employer, the State of New York, as part of an insurance offering to which Plaintiff Clark did not subscribe.

14. Plaintiff Clark received a notification from Excellus on October 8, 2015, informing him that his PII was compromised as a result of the data breach. Consequently, Plaintiff faces an ongoing, imminent, and impending threat of future additional harm from the theft of his PII, like all members of the proposed Class.

15. Defendant, Excellus is a New York not-for-profit corporation registered with the New York Department of State to conduct business in New York. Excellus' principal place of business is located at 165 Court Street, Rochester, NY.

JURISDICTION AND VENUE

16. This Court has original jurisdiction of this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class Members, the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and because there is diversity because at least one member of the class is a citizen of a state other than New York. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. §§1331 and 1367.

17. This Court has personal jurisdiction over Defendant because Excellus maintains its principal place of business in this District and is authorized to do business in New York and does conduct business in New York.

18. Venue is proper in this District pursuant to 28 U.S.C. §1391 as Defendant is headquartered in this District, and many of the unlawful acts or omissions are alleged to have occurred in this District.

FACTUAL BACKGROUND

19. Beginning on or about September 9, 2015, Excellus made the first in a series of announcements admitting that a massive data breach affected the PII of an estimated 10 million

of its subscribers. On that date, Excellus posted the following “Message from President and CEO, Christopher C. Booth” on its website and on the site excellusfacts.com:

Our investigation determined that the attackers may have gained unauthorized access to individuals’ information, which could include name, date of birth, Social Security number, mailing address, telephone number, member identification number, financial account information and claims information. This incident also affected members of other Blue Cross Blue Shield plans who sought treatment in the 31 county upstate New York service area of Excellus BCBS. Individuals who do business with us and provided us with their financial account information or Social Security number are also affected.

20. Excellus also began notifying many of its affected subscribers and non-customers of the breach by email dated September 9, 2015.

21. As a provider or health insurance, Excellus knew or should have known of the risks its subscribers, and non-subscribers faced when their PII was compromised, and of the need for Excellus to carefully safeguard that information.

22. Excellus acknowledges as much in a “Compliance Notice” that states:

We know how important your privacy is to you. Therefore, we are committed to protecting any personal information that you provide us...according to applicable laws, regulations and accreditation standards and practices, and we continue to evaluate new administrative, technical and physical safeguard for protecting your information.

23. Excellus’ “Privacy Policy,” effective April 14, 2003, also acknowledged Excellus’ obligation to detect and prevent security breaches.

24. Subscribers to Excellus’ health care services, and non-subscribers who provided their PII to Excellus, such as Plaintiff and the members of the proposed Class, rely on Excellus to maintain their PII in way that insures its privacy and security.

25. Notwithstanding, by no later than December 23, 2013, cyber-criminals were able to gain unauthorized access to the PII of millions of Excellus records. .

26. Excellus delayed announcing that it had discovered the data breach by nearly a month after it learned of it.

27. According to Mike Hamilton, VP Products at Ziften, in a September 29, 2015 article in *Health IT Outcomes*, “[t]he Excellus breach is just the latest example of how hackers are able to avoid detection and go unnoticed within a network for long periods of time. While the exact details of how the breach occurred have not yet been released, *the responsibility still lies with the hacked organization to do a better job of quickly detecting and responding* to these types of attacks”. . . “No attack should go undetected for extended lengths of time, in this case will over a year. Security teams need to shore up their existing security infrastructure with tools designed to provide the intelligence required to shut these hackers down and limit the damage.”

28. The health care industry presents a uniquely appealing target for data thieves. As *The New York Times* reported in a February 5, 2015 article, “[t]he threat of a hacking is particularly acute in the health care and financial services industry, where companies routinely keep the most sensitive personal information about their customers on large databases.”

29. Moreover, on April 8, 2014, the FBI’s Cyber Division issued a “Private Industry Notification” titled, “Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain,” that warned all healthcare providers that “[c]yber actors will likely increase cyber intrusions against health care systems . . . due to . . . lax cybersecurity standards, and a higher financial payout for medical records in the black market.”

30. Indeed, a PriceWaterhouseCoopers’ study found information security incidents rose by 60 percent in the health-care industry in 2014.

31. The FBI’s Private Industry Notification further reported: A SANS [Institute] report dated February 2014, indicated that health care security strategies and practices are poorly

protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property.... The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.

32. According to a U.S. Government Accountability Office's ("GAO") June 2007 report on data breaches, the consequences of medical identity theft are far greater than other types of identity theft:

In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health endangered by inaccurate entries in their medical records. This inaccurate information can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that a theft has occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or they attempt to seek medical care themselves, only to discover that they have reached their coverage limits.

33. Defendant stored the PII of Plaintiff and the members of the proposed Class in an inadequately protected/guarded/secured electronic or physical location.

34. Defendant designed and implemented its policies and procedures regarding the security of client PII. Those policies and procedures failed to adhere to reasonable and best industry practices in safeguarding the PII of Plaintiff and the proposed Class members.

CLASS ACTION ALLEGATIONS

35. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of FED. R. CIV. P. 23(a), 23(b)(2), and 23(b)(3) are met with respect to the Class defined below.

36. Plaintiff brings this action as a national class action for himself and all members of the following Class of similarly situated persons:

All persons in the United States whose PII was compromised as a result of the data breach announced by Excellus on or about September 9, 2015.

37. In addition to the national class defined above, Plaintiff brings this action on behalf of a New York subclass defined as:

All persons in New York whose PII was compromised as a result of the data breach announced by Excellus on or about September 9, 2015.

38. Excluded from the Class are Defendant, officers, directors, and employees of Defendant, any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

39. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

40. All members of the proposed Class are readily ascertainable, as Excellus has access to addresses and other contact information for all Class members, which can be used for providing notice to Class members.

41. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Excellus has admitted it includes approximately 10 million subscribers and non-subscribers nationwide. Accordingly, many of those persons are located in New York as Excellus operates in New York. Thus, the proposed Class is so numerous that joinder is impracticable.

42. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

- a) whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- b) whether Defendant's conduct was unlawful;
- c) whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect Class members' PII;
- d) whether Defendant unlawfully used, maintained, lost, or disclosed Class members' PII;
- e) whether Defendant unreasonably delayed in notifying affected subscribers of the security breach;
- f) whether Excellus' conduct violated New York law;
- g) whether Excellus knew or should have known that its computer systems were vulnerable to attack;
- h) whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- i) whether the two years identity theft protection Defendant offered to affected persons is sufficient;
- j) whether Plaintiff and other Class members are entitled to recover damages; and
- k) whether Plaintiff and other Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

43. **Typicality.** Plaintiff's claims are typical of the claims of the Class in that the representative Plaintiff, like all Class members, had his PII compromised and stolen. Plaintiff and

all Class members were injured through the uniform misconduct of Defendant described in this Complaint and assert the same claims for relief.

44. ***Adequacy.*** Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in class action and complex litigation, including in data breach litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of the Class. As a result, Plaintiff is knowledgeable on the subject matter alleged herein and well-suited to protect the interests of the Class.

45. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

46. ***Superiority.*** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class. Plaintiff and other Class members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation arising from the same data breaches. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

47. Class certification, therefore, is appropriate under FED. R. CIV. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual Class members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

48. Class certification is also appropriate under FED. R. CIV. P. 23(b)(2), in that Defendant has acted in a manner that applies generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate for the Class.

COUNT I

NEGLIGENCE

49. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

50. Excellus owed its subscribers and non-subscribers from whom it collected PII a duty to use reasonable care in the handling and safeguarding of their PII entrusted to Defendant.

51. By collecting Plaintiff and other Class members' PII, Defendant assumed a duty to use reasonable care to safeguard and protect their PII from being compromised or improperly disclosed to unauthorized third parties.

52. Excellus also had a duty to timely inform Plaintiff and other Class members that their PII had been compromised or improperly furnished to unauthorized third parties.

53. Defendant, through the acts described herein, breached its duty of care by:

- a. failing to properly implement and maintain adequate security measures to protect customer and non-customer PII from being accessed, disseminated, and misused by unauthorized third parties;
- b. failing to adequately store Plaintiff's and the other Class Members' PII; and
- c. failing to timely and sufficiently notify Plaintiff and other Class members that their PII had been compromised or improperly accessed by unauthorized third parties.

54. As a result, Plaintiff and other Class members have suffered or will suffer damages as the result of Excellus' negligence.

COUNT II

VIOLATION OF NY GEN. BUS. LAW § 349 ("NYGBL")

55. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

56. Excellus' business acts and practices and conduct/omissions alleged herein constitute deceptive acts or practices under the NYGBL.

57. At all relevant times, the challenged behavior of Excellus was consumer-oriented within the meaning of the NYGBL.

58. The practices of Excellus, as alleged herein, violated the NYGBL for, *inter alia*, one or more of the following reasons:

a. Excellus engaged in deceptive, unfair and unconscionable commercial practices which did, or tended to, mislead Plaintiff about facts that could not be reasonably known by him;

b. Excellus failed to reveal material facts to Plaintiff and the Class members;

c. Excellus made material misrepresentations and statements, or made material omissions of fact to Plaintiff and the Class members;

d. Under all of the circumstances, Excellus' conduct in employing these unfair and deceptive trade practices was malicious, willful, wanton, and outrageous such as to shock the conscience of the community and warrant imposition of punitive damages.

59. Excellus' violations of the NYGBL caused injuries to Plaintiff and Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully request the following relief:

- A. That the Court certify this case as a class action and appoint the named Plaintiff to be Class representatives and their counsel to be Class counsel;
- B. That the Court award Plaintiff appropriate relief, to include actual and statutory damages, disgorgement, and restitution;
- C. That the Court award Plaintiff preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law, including but not limited to the provision of credit and identity theft protection for the life of the victim;
- D. That the Court enter such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations alleged herein;
- E. That the Court impose punitive damages under any provision of law under which punitive damages may be imposed;
- F. That the Court award Plaintiff such other, favorable relief as may be available and appropriate under law or at equity;
- G. That the Court award costs and reasonable attorneys' fees; and
- H. That the Court enter such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 23, 2015

Respectfully submitted,

/s/ Jason J. Kane

Jason J. Kane (NY BAR No. 4561908)

Peiffer Rosca Wolf

Abdullah Carr & Kane,

A Professional Law Corporation

15 Fishers Road

Suite 111

Pittsford, New York 14534

T 585-310-5140

F 888-411-0038

jkane@prwlegal.com

Alan L. Rosca
Pro hac vice to be submitted
Peiffer Rosca Wolf
Abdullah Carr & Kane,
A Professional Law Corporation
1422 Euclid Avenue
Suite 1610
Cleveland, Ohio 44115
T 216-589-9280

Mark S. Goldman
Pro hac vice to be submitted
Paul J. Scarlato
Pro hac vice to be submitted
Brian D. Penny (NY BAR No. 4820106)
Douglas J. Bench
Pro hac vice to be submitted
GOLDMAN SCARLATO & PENNY, PC
101 E. Lancaster Avenue, Suite 204
Wayne, PA 19087
T (484) 342-0700
F (484) 580-8747
goldman@lawgsp.com
scarlato@lawgsp.com
penny@lawgsp.com
bench@lawgsp.com

Counsel for Plaintiff and the Proposed Class